UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/086,516	02/28/2002	Khanh V. Nguyen	50325-0644	2155

29989 7590 11/22/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/086,516	**Applicant(s)** NGUYEN ET AL.	
	Examiner Eleni A. Shiferaw	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 02 September 2005.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-29 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's arguments with respect to claims 1-29, filed on September 2, 2005, have been fully considered but they are not persuasive. The examiner would like to point out that this action is made final (MPEP 706.07a).

Response to Arguments

2. Applicant argues that:

a. Independent claims 1, 24, 26, and 28 are not taught by the references to include wherein *"selecting a subset from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol"* (section I, and page 6 par. 5).

b. The references, whether alone or in combination, fail to support claims 1, 14, 24-29 limitations wherein *"determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads and/or a secret integer unique for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads"* (section II and page 7 par. 2-5).

c. The references, whether alone or in combination, fail to support claims 1, 14, 24-29 limitations wherein *"sending a clue information to determine, only at the client and the server, the secret integer that is unique for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads for decrypting encrypted data."* (section III, and page 7 par. 2-5)

d. Dougall is not a valid reference under 35 U.S.C. 120 because applicants have not found no specific reference in Dougall claiming priority to the earlier filed date application. (page 8-9)

e. Dependent claims 2-13, and 15-23 are allowable based upon their dependency on allowable claims 1 and 14.

However, Examiner disagrees with applicant.

Regarding argument (a), Argument is not persuasive. Dougall teaches a set of data (digital audio-video signal) to be communicated between the client and source nodes. The data is compressed and well-known plurality of payloads/headers is disclosed. The plurality of **payloads are selected from a set of data and encrypted** (par. 0134-0135, 0074, fig. 20 element 915, fig. 3 elements 112, 8, 20, and 114).

Regarding argument (b), Argument is not persuasive. As described above in (a), Dougall teaches plurality of payloads (please see argument (a) above). Quick teaches a unique secrete integer/key by generating random number and concatenating the generated random number with public key (col. 3 lines 4-6, and col. 7 lines 6-8). Sufficient motivation to combine the teachings of Quick and Dougall is provided in the first Office Action page 3.

Regarding argument (c), Argument is not persuasive. Dougall teaches multiple clue information. For example: index field, authentication value, authentication length field and etc ... The client node receives clue information/key index field to determine the key used to encrypt the packet and decrypt the encrypted packet (par. 0134-0137). Unique secrete integer/key is described above in (b).

Regarding argument (d), Argument is not persuasive. The office has reviewed the appropriate requirements during filing before publishing Dougall's reference. The priority date of Dougall's is correct and applicant is provided a copy of Dougall's request to the office for proper priority date of September 12, 2001, under 37 C.F.R. 1.120. Moreover the information on the continuation application No. 09/950,927 is the same as the publication. Therefore the priority date of September 12, 2001 is appropriate and the rejection is still maintained.

Regarding argument (e), examiner disagrees with applicant. Based on the arguments set forth by the examiner for arguments (a), (b), (c), and (d), the dependent claims stand rejected.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. Therefore, the examiner asserts that the system of the prior art, Dougall and Quick teach or suggest the subject matter as recited in independent claims 1, 14, and 24-29. Dependent claims 2-13, and 15-23, are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action dated November 14, 2005. Accordingly, rejections for claims 1-29 are respectfully maintained.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1-7, 11-15, 17-19, and 22-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dougall et al. (Dougall, Pub. No.: US 2003/0093485 A1) in view of Quick, Jr. (Quick, Patent No.: US 6,260,147 B1).

As per claims 1, 24, and 26, Dougall teaches a method/medium/apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transfer protocol, the method comprising the computer-implemented steps of:

selecting a subset from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol (Dougall page 12 par. 0135, and fig. 20 element 915); and

sending, from a sending device of the client and the server to a receiving device of the client and the server, in the particular payload, the encrypted data and clue information to determine, only at the client and the server, the secrete integer (key) for decrypting the encrypted data (Dougall page 12 lines 0135-page 13 par. 0137, and fig. 20 elements 920, 914, & 919);

Dougall fails to teach:

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads; and

based on the subset and the secret integer, generating encrypted data that

is impractical for a device other than the client and the server to decrypt;

However **Quick** discloses:

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads (col. 3 lines 4-6, and col. 7 lines 6-8); and

based on the subset and the secret integer, generating encrypted data that

is impractical for a device other than the client and the server to decrypt (col. 5 lines 9-25). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Quick within the system of Dougall because they are analogous in securing data transmitted over a network (Quick fig. 1). One would have been motivated to incorporate the teachings of Quick within Dougall because it would further enhance security (Quick col. 5 lines 26-33).

As per claims 14, 25, and 27, Dougall teaches a method/medium/apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload associated with the transport protocol, the method comprising the computer-implemented steps of:

receiving, at a receiving device of the client and the server from a sending device of the client and the server, in a particular payload of the unencrypted transfer protocol, encrypted data and clue information to determine, only at the client and the server, a secret integer (key) unique for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads (Dougall page 12 lines 0135-page 13 par. 0137, and fig. 20 elements 920, 914, & 919);

Dougall fails to teach:

determining the secret integer based, at least in part, on the clue information; and

based on the secret integer, decrypting the encrypted data to generate a subset of data to be communicated between client and server.

However **Quick** discloses:

determining the secret integer based, at least in part, on the clue information (col. 3 lines 4-6, and col. 7 lines 6-8); and

based on the secret integer, decrypting the encrypted data to generate a subset of data to be communicated between client and server (col. 5 lines 9-25). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Quick within the system of Dougall because they are analogous in securing data transmitted over a network (Quick fig. 1). One would have been motivated to incorporate the teachings of Quick within Dougall because it would further enhance security (Quick col. 5 lines 26-33).

As per claim 28, Dougall teaches an apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, comprising:

a network interface that is coupled to the data network for sending one or more packet flows thereto (Dougall page 4 par. 0060);

a processor (Dougall page 2 par. 0030);

one or more stored sequences of instructions which, when executed by the

processor (Dougall page 2 par. 0030), cause the processor to carry out the steps of:

selecting a subset from a set of data to be communicated between the client

and the server in a particular payload of the unencrypted transfer protocol (Dougall page 12 par. 0135, and fig. 20 element 915); and

sending, to a receiving device of the client and the server, in the particular

payload, the encrypted data and information to determine, only at the client and the server, the secret integer (key) for decrypting the encrypted data (Dougall page 12 lines 0135-page 13 par. 0137, and fig. 20 elements 920, 914, & 919).

Dougall fails to teach:

determining a secret integer that is unique for the subset among a plurality of

subsets in a plurality of payloads;

based on the subset and the secret integer, generating encrypted data that is practically unintelligible to a device other than the client and the server;

However **Quick** discloses:

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads (col. 3 lines 4-6, and col. 7 lines 6-8); and

based on the subset and the secret integer, generating encrypted data that is impractical for a device other than the client and the server to decrypt (col. 5 lines 9-25). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Quick within the system of Dougall because they are analogous in securing data transmitted over a network (Quick fig. 1). One would have been motivated to incorporate the teachings of Quick within Dougall because it would further enhance security (Quick col. 5 lines 26-33).

As per claim 29, Dougall teaches an apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom (Dougall page 4.par. 0060);

a processor (Dougall page 2 par. 0030);

one or more stored sequences of instructions which, when executed by the processor (Dougall page 2 par. 0030), cause the processor to carry out the steps of:

receiving, from a sending device of the client and the server, in a particular payload of the unencrypted transfer protocol, encrypted data and information to determine, only at the client and the server, a secret integer (key) unique for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads (Dougall page 12 lines 0135-page 13 par. 0137, and fig. 20 elements 920, 914, & 919);

Dougall fails to teach:

determining the secret integer based, at least in part, on the information; and

based on the secret integer, decrypting the encrypted data to generate a subset of data to be communicated between client and server.

However **Quick** discloses:

determining the secret integer based, at least in part, on the information (col. 3 lines 4-6, and col. 7 lines 6-8); and

based on the secret integer, decrypting the encrypted data to generate a subset of data to be communicated between client and server (col. 5 lines 9-25). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Quick within the system of Dougall because they are analogous in securing data transmitted over a network (Quick fig. 1). One would have been motivated to incorporate the teachings of Quick within Dougall because it would further enhance security (Quick col. 5 lines 26-33).

As per claims 2 and 15, Dougall and Quick teach all the subject matter as described above. In addition, Dougall teaches a method, wherein the unencrypted transfer

protocol is Hypertext Transfer Protocol (HTTP) (Dougall page 7 par. 0094).

As per claim 3, Dougall and Quick teach all the subject matter as described above. In addition, Quick teaches a method, said step of determining a secret integer that is unique for the subset further comprising the steps of:

generating a first integer using a random number generator (col. 3 lines 4-6, and col. 7 lines 6-8);

determining a shared secret key to be shared with the receiving device based on the first integer and a first public key associated with the receiving device (col. 3 lines 4-6, and col. 7 lines 6-8); and

selecting the secret integer based on the shared secret key (col. 3 lines 4-6, and col. 7 lines 6-8). The rational for combining are the same as claim 1 above.

As per claim 4, Dougall and Quick teach all the subject matter as described above. In addition, Quick teaches a method, said step of sending the information to

determine the secret integer further comprising the steps of determining a second public key associated with the sending device based on the first integer (Quick col. 7 lines 14-15); and including the second public key in the information to determine the secret integer (Quick col. 7 lines 14-15). The rational for combining are the same as claim 1 above.

As per claim 5, Dougall and Quick teach all the subject matter as described above. In addition, Quick teaches a method, said step of sending the information to

determine the secret integer further comprising the steps of determining a plurality of second public keys associated with the sending device based on the first integer, wherein each of the second public keys is associated with one of a plurality of subsets from the set of data (Quick col. 7 lines 14-15); and

including the plurality of second public keys in the information to determine the secret integer (Quick col. 7 lines 14-15). The rational for combining are the same as claim 1 above.

As per claim 6, Dougall and Quick teach all the subject matter as described above. In addition, Dougall teaches a method, said step of setting the secret integer further comprising the step of applying a particular hash function to the shared secret key to generate the secret integer (page 12 par. 0136).

As per claim 7, Dougall and Quick teach all the subject matter as described above. In addition, Quick teaches a method, said step of generating encrypted data further comprising the step of performing an exclusive or (XOR) operation between corresponding bits of the subset and the secret integer to generate the encrypted data (Quick col. 7 lines 14-16).

As per claim 11, Dougall and Quick teach all the subject matter as described above. In addition, Quick teaches a method, further comprising, before said step of determining the secret integer, performing the steps of

determining the shared secret key based on a particular communication between the client and the server (Quick col. 5 lines 9-25); and

storing the shared secret key in a secure data structure (Quick col. 4 lines 47-58).

As per claims 12 and 23, Dougall and Quick teach all the subject matter as described above. In addition, the combination of Dougall and Quick teach a method, wherein the secret integer has a particular number of bits fixed for all subsets in all payloads communicated during a communication session between the client and the server (Dougall page 12 par. 0135, and Quick col. 8 lines 18-20).

As per claim 13, Dougall and Quick teach all the subject matter as described above. In addition, the combination of Dougall and Quick teach teaches a method, wherein the secret integer has a number of bits that varies in accordance with lengths of payloads that are communicated during a communication session between the client and the server (Dougall page 12 par. 0135, and Quick col. 8 lines 18-20).

As per claim 17, Dougall and Quick teach all the subject matter as described above. In addition, the combination of Dougall and Quick teach a method, said step of generating the secret integer further comprising the step of applying a particular hash function to the shared secret key to generate the secret integer (Dougall page 12 par. 0136, and Quick page 5 par. 0093).

As per claim 18, Dougall and Quick teach all the subject matter as described above. In addition, Quick teaches a method, wherein:

the method further comprises the steps of

determining a shared secret key based on a particular communication between the client and the server (Quick col. 5 lines 9-25), and

storing the shared secret key in a secure data structure (Quick col. 4 lines 47-58); and the clue information indicates a number of times a particular hash function is applied to the shared secret key in generating the secret integer (Quick page 5 par. 0093; n).

As per claim 19, Dougall and Quick teach all the subject matter as described above. In addition, Quick teaches a method, said step of determining the secret integer further comprising the step of causing the particular hash function to be applied the number of times indicated by the clue information to the shared secret key (Quick page 5 par. 0093).

As per claim 22, Dougall and Quick teach all the subject matter as described above. In addition, Quick teaches a method, said step of decrypting the encrypted data further comprising the step of performing an exclusive or (XOR) operation between corresponding bits of the encrypted data and the secret integer to generate the subset

of data (Quick col. 7 lines 14-16).

5. Claims 8-10, 16, and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dougall et al. (Dougall, Pub. No.: US 2003/0093485 A1) in view of Quick, Jr. (Quick,

Patent No.: US 6,260,147 B1), and further in view of Carman et al. (Carman, Pub. No.: US 2002/0199102 A1).

As per claim 8, Dougall and Quick teach all the subject matter as described above. However Dougall and Quick fail to explicitly teach applying a particular hash function a plurality of times to a shared secret key;

However Carman teaches a method, wherein: said step of determining the secret integer further comprises the step of applying a particular hash function a plurality of times to a shared secret key shared with the receiving device (Carman page 5 par. 0093); and

said step of sending the information to determine the secret integer further comprises the step of storing, as part of the clue information, data that indicates a

number of times the particular hash function has been applied (Carman page 5 par. 0093; n). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Carman within the combination system of Dougall and Quick because it would securely communicate nodes.

As per claims 9-10, and 21, Dougall, Quick, and Carman teach all the subject matter as described above. In addition the combination of Quick and Carman teach a method, said step of determining the secret integer further comprising the steps of:

determining a first integer formed after the particular hash function is applied the number of times indicated in the information (Carman page 5 par. 0093, and Quick col. 3 lines 4-6, and col. 7 lines 6-8);

determining a second integer formed after the particular hash function is applied fewer times than the number of times indicated in the information (Carman page 5 par. 0093, and Quick col. 3 lines 4-6, and col. 7 lines 6-8);

function is different from the particular hash function that is used to determine the first integer (Carman page 5 par. 0093); and

performing an exclusive or (XOR) operation between corresponding bits of the first integer and the second integer (Quick col. 7 lines 14-16).

As per claim 16, Dougall, Quick, and Carman teach all the subject matter as described above. In addition the combination of Quick and Carman teach teaches a method, said step of determining the secret integer further comprising the steps of:

based on the clue information, determining a shared secret key shared with the sending device (Carman page 5 par. 0093; n); and

generating the secret integer bored on the shared secret key (Quick col. 3 lines 4-6 and col. 7 lines 6-9).

As per claim 20, Dougall, Quick, and Carman teach all the subject matter as described above. In addition the combination of Quick and Carman teaches a method, said step of determining the secret integer further comprising the steps of:

determining a first integer formed after the particular hash function is applied the number of times indicated by the clue information (Carman page 5 par. 0093, and Quick col. 3 lines 4-6, and col. 7 lines 6-8);

determining a second integer formed after the particular hash function is applied fewer times than the number of times indicated by the clue information (Carman page 5 par. 0093, and Quick col. 3 lines 4-6, and col. 7 lines 6-8); and

performing an exclusive or (XOR) operation between corresponding bits of the first integer and the second integer (Quick col. 7 lines 14-16).

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E. S.
November 14, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100